

INFORMATION PROCESSING DEVICE

Publication number: WO0057278 (A1)

Publication date: 2000-09-28

Inventor(s): KITAHARA JUN [JP]; ASAHI TAKESHI [JP]; OWADA TORU [JP]

Applicant(s): HITACHI LTD [US]; KITAHARA JUN [JP]; ASAHI TAKESHI [JP]; OWADA TORU [JP]

Classification:

- **international:** G06F21/00; G06F12/14; G11B20/00; G06F21/00; G06F12/14; G11B20/00; (IPC1-7): G06F12/14; G06F3/06; G06F15/78; G11B20/10

- **European:** G06F21/00N1V3; G06F21/00N1C; G06F21/00N1C1

Application number: WO2000JP01333 20000306

Priority number(s): WO1999/JP01402 19990319

Also published as:

 US7082539 (B1)

JP3975677 (B2)

WO0057290 (A1)

Cited documents:

JP5053921 (A)

JP1041947 (A)

JP4163768 (A)

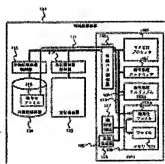
JP9044407 (A)

JP4149652 (A)

[more >>](#)

Abstract of WO 0057278 (A1)

A device structure for reliably encrypting and decrypting information is provided, which is used for security with information processing device, a communication device and a file management device. Such devices comprise a plurality of semiconductor parts. Therefore, confidential data may remain in devices, for example, in a system bus and semiconductor memory for main storage. To solve this problem, a device CPU is equipped with a microprocessor, an encryption algorithm ROM, an encryption hardware, RAM, a key storage area, and an external bus control, which are all integrated into a single semiconductor chip. Encryption and decryption take place only within the CPU, and the internal operations of the CPU cannot be inferred from signals outside the CPU.



```

001... INFORMATION PROCESSING CENTER
002... MAIN DECK
003... CONTROL STATION
004... INFORMATION
005... DISPLAY FLIGHT
006... FLIGHT INFORMATION
007... FLIGHT INFORMATION
008... FLIGHT
009... FLIGHT
010... FLIGHT
011... FLIGHT
012... FLIGHT
013... FLIGHT
014... FLIGHT
015... FLIGHT
016... FLIGHT
017... FLIGHT
018... FLIGHT
019... FLIGHT
020... FLIGHT
021... FLIGHT
022... FLIGHT
023... FLIGHT
024... FLIGHT
025... FLIGHT
026... FLIGHT
027... FLIGHT
028... FLIGHT
029... FLIGHT
030... FLIGHT
031... FLIGHT
032... FLIGHT
033... FLIGHT
034... FLIGHT
035... FLIGHT
036... FLIGHT
037... FLIGHT
038... FLIGHT
039... FLIGHT
040... FLIGHT
041... FLIGHT
042... FLIGHT
043... FLIGHT
044... FLIGHT
045... FLIGHT
046... FLIGHT
047... FLIGHT
048... FLIGHT
049... FLIGHT
050... FLIGHT
051... FLIGHT
052... FLIGHT
053... FLIGHT
054... FLIGHT
055... FLIGHT
056... FLIGHT
057... FLIGHT
058... FLIGHT
059... FLIGHT
060... FLIGHT
061... FLIGHT
062... FLIGHT
063... FLIGHT
064... FLIGHT
065... FLIGHT
066... FLIGHT
067... FLIGHT
068... FLIGHT
069... FLIGHT
070... FLIGHT
071... FLIGHT
072... FLIGHT
073... FLIGHT
074... FLIGHT
075... FLIGHT
076... FLIGHT
077... FLIGHT
078... FLIGHT
079... FLIGHT
080... FLIGHT
081... FLIGHT
082... FLIGHT
083... FLIGHT
084... FLIGHT
085... FLIGHT
086... FLIGHT
087... FLIGHT
088... FLIGHT
089... FLIGHT
090... FLIGHT
091... FLIGHT
092... FLIGHT
093... FLIGHT
094... FLIGHT
095... FLIGHT
096... FLIGHT
097... FLIGHT
098... FLIGHT
099... FLIGHT
100... FLIGHT

```

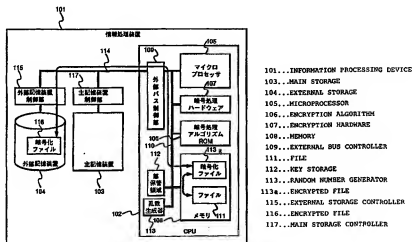
Data supplied from the *esp@cenet* database — Worldwide



(51) 国際特許分類7 G06F 12/14, 15/78, 3/06, G11B 20/10	A1	(11) 国際公開番号 WO00/57278 (43) 国際公開日 2000年9月28日(28.09.00)
(21) 国際出願番号 PCT/JP00/01333 (22) 国際出願日 2000年3月6日(06.03.00) (30) 優先権データ 特願平PCT/JP99/01402 1999年3月19日(19.03.99) JP (71) 出願人 (米国を除くすべての指定国について) 株式会社 日立製作所(HITACHI, LTD.)(JP/JP) 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo, (JP) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ) 北原 潤(KITAHARA, Jun)(JP/JP) 朝日 猛(ASAHI, Takeshi)(JP/JP) 大和田徹(OWADA, Toru)(JP/JP) 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP) (74) 代理人 弁理士 作田康夫(SAKUTA, Yasuo) 〒100-8220 東京都千代田区丸の内一丁目5番1号 株式会社 日立製作所内 Tokyo, (JP)		(81) 指定国 CN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE) 添付公開書類 国際調査報告書

(54)Title: INFORMATION PROCESSING DEVICE

(54)発明の名称 情報処理装置



(57) Abstract

A device structure for reliably encrypting and decrypting information is provided, which is used for security with information processing device, a communication device and a file management device. Such devices comprise a plurality of semiconductor parts. Therefore, confidential data may remain in devices, for example, in a system bus and semiconductor memory for main storage. To solve this problem, a device CPU is equipped with a microprocessor, an encryption algorithm ROM, an encryption hardware, RAM, a key storage area, and an external bus control, which are all integrated into a single semiconductor chip. Encryption and decryption take place only within the CPU, and the internal operations of the CPU cannot be inferred from signals outside the CPU.

本発明は、秘密保持のために、情報を暗号化／復号化する情報処理装置や通信装置やファイル管理装置において、安全に暗号化／復号化を行う装置構成を提供するものである。

これらの装置は、複数の半導体部品から構成されている。そのため、装置内のシステムバスや主記憶を構成する半導体記憶素子に秘密にすべきデータが存在してしまう問題点がある。

そこで、本発明は以下の構成をとる。各装置のCPUに、マイクロプロセッサと、暗号処理アルゴリズムROMと、暗号処理ハードウェアと、RAMと、鍵保管領域と、外部バス制御部を設けさらに同一半導体チップ上に集積する。このCPUを内でのみ暗号化／復号化処理を行い、さらにCPU内部動作をCPU外部信号から推測不可能にする。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AG アンティグア・バーブーダ	DZ アルジェリア	LC セントルシア	SD スーダン
AL アルバニア	EE エストニア	LI リヒテンシュタイン	SE スウェーデン
AM アルメニア	ES スペイン	LK スリ・ランカ	SG シンガポール
AT オーストリア	FI フィンランド	LR リベリア	SI スロヴェニア
AU オーストラリア	FR フランス	LS レソト	SK スロヴァキア
AZ アゼルバイジャン	GA ガボン	LT リトアニア	SL シェラ・レオネ
BA ボスニア・ヘルツェゴビナ	GB 英国	LU ルクセンブルグ	SN セネガル
BB バルバドス	GD グレナダ	LV ラトヴィア	SZ スワジランド
BE ベルギー	GE ギルジャ	MA モロッコ	TD チャド
BF ブルキナ・ファソ	GH ガーナ	MC モナコ	TG トーゴ
BG ブルガリア	GM ガンビア	MD モルドヴァ	TJ タジキスタン
BJ ベナン	GN ギニア	MG マダガスカル	TM トルクメニスタン
BR ブラジル	GR ギリシャ	MK マケドニア旧ユーゴスラヴィア	TR トルコ
BY ベラルーシ	HR クロアチア	ML マリ	TT トリニダード・トバゴ
CA カナダ	HU ハンガリー	MN モンゴル	TZ タンザニア
CF 中央アフリカ	ID インドネシア	MR モーリタニア	UA ウクライナ
CG コンゴ	IE アイルランド	MW マラウイ	UG ウガンダ
CI コートジボアール	IL イスラエル	MX メキシコ	US 米国
CM カメルーン	IN インド	MZ モザンビーク	UZ ウズベキスタン
CN 中国	IS アイスランド	NE ニジェール	VN ヴェトナム
CU キューバ・リカ	IT イタリア	NL オランダ	YA ユーゴスラヴィア
CY キプロス	JP 日本	NO ノルウェー	ZW 南アフリカ共和国
CZ チェコ	KE ケニア	NZ ニュージーランド	
DE ドイツ	KG キルギスタン	PL ポーランド	
DK デンマーク	KP 北朝鮮	PT ポルトガル	
	KR 韓国	RO ルーマニア	

明 細 書

情報処理装置

5

技術分野

本発明は、情報の保管、転送時の秘密性を保つために暗号を使用する情報処理装置に関する。その中でも特に、秘密性保持の高い情報処理を構築することに関する。

10

背景技術

暗号を使用する情報処理装置の従来技術としては、以下のものがある。

ハードディスクドライブのような外部記憶装置に、情報を暗号化して記憶するものとして、特開平10-275115号公報がある。特開平10-275115号公報では、外部記憶装置12に一旦書き込まれた暗号化データY_a、Y_bを情報端末装置11へ転送する過程で、暗号化・復号鍵蓄積部35に蓄積された復号鍵K_bを用いながら当該暗号化データY_a、Y_bに逐次的に復号処理を施すものである。

また、情報処理装置内に専用の暗号処理装置を設けたものとして、特開平10-214233号公報がある。特開平10-214233号公報では、携帯型PCの中にデータを暗号化して暗号化ファイルのボディ部を生成する暗号化装置を備えている。

ここで、暗号化や復号化といった暗号処理は、一般に主記憶上のデータを対象に処理するため、主記憶上に秘密にすべきデータが存在する。情報を暗号化するためには、暗号アルゴリズムに従い情報を処理しなければならないが、暗号アルゴリズムと暗号に用いる鍵情報と暗号をかける秘密情

25

報全てを、安全に処理する必要が生じる。

しかし、これらの従来技術では以下の問題が存在する。

従来技術においては、秘密情報や暗号処理の途中経過が主記憶上に存在するため、幾つかの手法で情報を取り出す事が可能になる問題がある。この問題は、CPUや主記憶などが、複数の半導体で構成されている情報処理装置において、CPUを用いて暗号処理を行うと暗号アルゴリズムや暗号をかける秘密情報や暗号処理の途中経過が主記憶上に存在するためである。

また、情報処理装置内には、情報処理装置を構成する各半導体部品を接続する信号線（例えばバス）が存在するため、この信号線を観察し、情報を解析する事により、暗号化する前のデータや復号化したデータを簡単に取り出せるという問題がある。

また、装置外部の信号線に対して暗号化したデータを送出するものとして、特開平2-297626があるが、暗号化するのに必要な鍵情報は外部から与えられており、この鍵情報の機密管理を確実に行わないと、データの暗号化が意味を成さなくなる問題がある。

発明の開示

従来技術の問題を解決するために、本発明では、以下の構成とした。

情報処理装置を構成する半導体内部で暗号化処理を施す。また、暗号化処理に必要な鍵情報も半導体内部で生成する。また、情報処理装置内の信号線の上に暗号に関する情報を出力しない。情報処理装置の信号線には、他者に観察されてもかまわない情報が出力される。この情報としては、暗号化された情報や暗号化する必要のない情報などである。なお、暗号に関する情報としては、暗号化されていない情報や暗号化された情報を復号するための情報を含む。

より具体的には、本発明の構成は、情報処理装置での処理を実行する処

理装置（CPU）と同一半導体チップに、RAM と暗号処理アルゴリズムと暗号処理ハードウェアと、鍵情報生成ハードウェアと、鍵情報格納ハードウェアを集積したものである。なお、本発明では便宜上 CPU と読んでいるが、名称はこれに限られず、情報処理装置を構成する半導体チップであればよい。その中でも特に、情報処理装置の制御や演算処理を行う処理装置がよい。つまり、本発明は、情報処理装置を構成する 1 半導体チップ内で鍵情報の生成を含め暗号化処理が閉じているものである。さらに、本発明では、CPU が複数個あり、それぞれにおいて、暗号化処理が行う構成としてもよい。

また、この暗号処理が内蔵する RAM 内で処理されてもよい。

また、CPU に内蔵される RAM を主記憶として用い、アプリケーションプログラムの実行も内蔵する RAM 内で処理されるものでもよい。

また、アプリケーションプログラム自体も暗号化され、外部記憶装置には、暗号化ファイルが存在する構成にしたものでもある。

また、外部バスへのデータ出力を制御する外部バス制御部を設けてもよい。この外部バス制御部では、内部 RAM がアクセスされているときのデータを外部バスへ出力しないよう制御してもよい。さらに、このデータ外部バスに出力してもよい情報が否かを判断して、出力してもよい場合にデータを外部バスに出力するように制御してもよい。

また、通信データの暗号化／復号化を CPU 内部で処理するものである。

さらに、これらのいずれかの構成によって、情報に応じて暗号化するか否かを決定してもよい。情報が、暗号化しなくともよい情報であれば暗号化せずに情報処理装置の信号線上に出力する構成としてもよい。

さらに、本発明は、ディスクシステムコントローラ内のプロセッサ内部で暗号処理を可能にすることで、磁気ディスク上のファイル配置情報を暗号化したものも含まれる。

図面の簡単な説明

第1図は、本発明の情報処理装置の構成を示す図である。第2図は、本
発明の情報処理装置におけるファイル生成を説明する図である。第3図は、
5 本発明の1形態である主記憶を内蔵するCPUを有する情報処理装置の構成
を示す図である。第4図は、本発明の1形態である外部記憶装置に格納し
ているアプリケーションプログラムをCPUで暗号化する情報処理装置の構
成を示す図である。第5図は、外部バス制御部の構成を示す図である。第
6図は、外部バス制御部で外部バスへのデータを出力させない1実施例を
10 説明する図である。第7図は、鍵生成に必要な乱数生成部の構成を示す図
である。第8図は、鍵保管部の構成を示す図である。第9図は、暗号化お
よび復号化する装置が自分自身である場合の暗号化複合化処理と鍵の関係
を示す図である。第10図は、第9図の鍵の取扱いを変え、記憶しなければ
ならない鍵情報を少なくする構成を示す図である。第11図は、暗号化
15 する装置と復号化する装置が異なる場合の、暗号化処理と鍵の関係、複
合化処理と鍵の関係を示す図である。第12図は、第11図に加えて、送信
者の保証情報を付加した構成を示す図である。第13図は、相手から入手
する鍵情報を認証する仕組みを示す図である。第14図は、本発明をプロ
セッサバスおよびシステム情報処理装置に適用した場合の構成を示す図で
20 である。第15図は、本発明を通信に適用した場合の構成を示す図である。
第16図は、外部記憶装置に本発明を適用した場合を説明する図である。
第17図は、第16図の構成で暗号化ファイル配置情報の書込みを説明す
る図である。第18図は、ディスクコントローラの構成を示す図である。
第19図は、本発明の1形態である複数のCPUを有する情報処理装置を示す
25 図である。第20図は、第19図の変形例を示す図である。第21図は、
第16図に示した構成の変形例である。第22図は、第16図に示した構

成の変形例である。第23図は、第15図に示す情報処理装置がネットワークに接続されている全体システムを表わす図である。

発明を実施するための最良の形態

5 以下、図面を用いて本発明の実施例を説明する。

まず、本発明の第一の実施例を第1図および第2図を用いて説明する。

第1図は、少なくとも、CPU(102)、主記憶装置(103)、外部記憶装置(104)を備える情報処理装置(101)の構成を模式的に表した図である。CPU(102)、主記憶装置制御部(117)、外部記憶装置制御部(115)は、理論上のシステムバス(114)で接続され、各々に主記憶装置(103)、外部記憶装置(104)が接続される。実際の信号線の接続は、第7図のようになるが、データの流れを理論的に考えると、模式的に第1図のように表す事が出来る。

CPU(102)は、マイクロプロセッサ(105)と、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)からなる。さらに、これらを同一半導体チップ上に集積する。

CPU(102)内部では、マイクロプロセッサバス(110)に、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、外部バス制御部(109)が接続される。本実施例においては、CPU内部でデータに対する暗号化処理が行われる。

ファイル(111)を暗号化するには、暗号処理アルゴリズムROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化する。この時の暗号化に用いる鍵データは、CPU(102)内で生成しても良いし、あらかじめ与えられるデータを用いても良い。但し、この鍵データはCPU(102)内の鍵保管領域(112)、保持されていなければならない。暗号化処理において、途中経過のデータが生成される場合は、その途中経過のデータもRAM(108)内

に格納する。このようにして、ファイル(111)から暗号化ファイル(113)を生成する。

暗号化ファイル(113)は、システムバス(114)を通して外部記憶装置制御部(115)を経由して外部記憶装置(104)に格納する。

5 外部記憶装置(104)に格納されている暗号化ファイル(116)を復号化する場合は、逆の順序で処理を行う。

まず、外部記憶装置(104)から暗号化ファイル(116)を外部記憶装置制御部(115)を経由して RAM(108)に読み込む。次に、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて復号化する。

10 大量のデータを高速に暗号化／復号化するためには、暗号鍵と復号鍵が共通である共通鍵暗号系を用いる。共通鍵暗号系では、暗号と復号は処理の順序が逆になっているだけで、最小単位の処理自体は暗号化も復号化も同じである。暗号処理アルゴリズム ROM(106)には、復号化処理の手順も格納しておく。また、暗号処理ハードウェア(107)は復号化でも使用する事が可能である。

15 第2図は、第1図のファイル(111)を生成するまでの過程を示したものである。

20 アプリケーションプログラム(201)は、稼動時以外は外部記憶装置内に格納されている。このアプリケーションプログラムに起動がかかると主記憶に展開され動作可能な状態になる。動作可能になったアプリケーションプログラム(202)は、オペレーティングシステム等への情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(203)として RAM(108)内の空間を割り当てる。

25 この状態で、アプリケーションプログラム(202)は、マイクロプロセッサ

(105)で処理され、生成された情報は作業領域(203)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

アプリケーションプログラム(202)自体は主記憶上に存在し、そのアプリケーションプログラムの作業領域(203)を RAM(108)上を取るためには、オペレーティングシステム等の情報処理装置管理プログラムが管理するマイクロプロセッサが持つメモリ管理機能を用い、アプリケーションプログラムの作業領域を示す論理アドレスを RAM(108)内の物理アドレスに変換する事で可能になる。

鍵保持部(112)は、RAM(108)の領域内に設けられていても良いが、不揮発性でなければならない。EEPROM や FlashROM のような不揮発性の ROM で構成しても良いし、バッテリーバックアップされた SRAM で構成しても良い。バッテリーバックアップされた SRAM で構成した場合、暗号に使用した鍵を取り出そうと、情報処理装置に攻撃が加えられた場合にそれを検知し、バックアップ電源を切断する事で、鍵情報を消失させ秘密情報を守ることも可能になる。

このように、情報の生成、暗号処理を同一半導体チップ内で行う事により、半導体チップの端子等の信号を観察するような解析方法でも、暗号のかからない秘密情報を入手する事は困難になる。

次に、本発明の第二の実施例を第3図を用いて説明する。

第3図は、CPU(101)内の RAM(108)を、情報処理装置(101)の主記憶として構成したものである。

この場合、外部記憶装置に格納されているアプリケーションプログラム(301)は、起動時に RAM(108)に展開され動作可能になる。動作可能になったアプリケーションプログラム(302)は、オペレーティングシステム等の情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。こ

のとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(303)として RAM(108)内の空間を割り当てる。この状態で、アプリケーションプログラム(302)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(303)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

生成されたファイル(111)は、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化される。暗号化されたファイル(113)は、外部記憶装置に暗号化ファイル(116)として格納される。

第3図では、CPU外部の主記憶装置を図示していないが、秘密情報を生成するアプリケーションプログラムとそれ以外のアプリケーションプログラムを区別し、秘密情報を生成するアプリケーションプログラムの実行は、RAM(108)で行い、それ以外のアプリケーションプログラムは、従来通りCPU外部の主記憶装置で処理する構成を取っても良い。

このように、RAM(108)を主記憶にする事により、CPU(102)外部にはアプリケーションプログラム(301)をRAM(108)に展開する時のデータ転送しか発生せず、アプリケーションプログラム自体の処理も安全に行える。

本発明の第三の実施例を第4図を用いて説明する。

本実施例では、暗号化されたアプリケーションプログラム(401)を外部記憶装置(104)に格納している。このアプリケーションプログラムは、情報処理装置のCPU内で復号化される。このため、バス(114)上には、復号化されたアプリケーションプログラムは出力されず、復号化されたアプリケーションプログラムはCPU内部で閉じている。このため、他者がこのアプリケーションプログラムを観察することを防止できる。

以下、第三の実施例の詳細を説明する。外部記憶装置内の暗号化アプリケーションプログラム(401)は、起動時にバス(114)を通して情報処理装置

5 内の RAM(108)に転送される。転送された暗号化アプリケーションプログラム(402)は、RAM(108)に展開される。展開された暗号化アプリケーションプログラム(402)は、RAM(108)内で復号化され、アプリケーションプログラム(403)になる。この状態でアプリケーションプログラム(403)が動作し、
RAM(108)内の作業領域(404)を用いながら情報を生成する。生成された情報は必要な部分が選択され、ファイル(111)としてまとめられる。ファイル(111)を暗号化し、暗号ファイル(113)を生成する。暗号ファイル(113)を暗号ファイル(116)として外部記憶装置(104)に格納する。

10 このように、アプリケーションプログラム自体も暗号化ファイルの一つとして外部記憶装置に格納する事により、さらに安全性を高める事も出来る。

なお、この暗号化アプリケーションプログラム(401)を生成するためには、アプリケーションプログラム自体をファイル(111)として、暗号化を行うものである。

15 次に、第5図および第6図を用いて、本発明の外部バス制御部の説明をする。

20 第一から第三の各実施例に用いられる外部バス制御部(109)は、CPU内部と外部とのデータの入出力を制御するものである。例えば、マイクロプロセッサ(105)が行う、暗号処理のために暗号処理アルゴリズムROM(106)又は、暗号処理ハードウェア(107)又は、RAM(108)へのアクセスをCPU(102)外部に出ないように制御する。但し、マイクロプロセッサ(105)のアクセスがCPU外部に出力されても構わないものであれば、外部に出力されるよう制御してもよい。この場合、CPU外部に出力されても構わないデータとしては、暗号処理を行わず他の情報処理装置に転送するデータなどがある。

25 外部バス制御部(501)は、マイクロプロセッサ(502)の制御バス(503)、アドレスバス(504)、データバス(505)と、CPUの外部へ出る外部制御バス

(506)、外部アドレスバス(507)、外部データバス(508)の間にあり、外部制御バス生成部(509)と、アドレス比較部(510)と、アドレス方向制御部(512)と、データ方向制御部(513)と、マスク信号生成部(511)と、信号マスク部(514)(519)から構成される。

5 制御バス(503)と外部制御バス(506)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等が通される。これらの信号によりバスサイクルが制御される。

外部制御バス生成部(509)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等を監視する。外部制御バス生成部(509)は、マイクロプロセッサがバスアクセス権を所有しているか否かを判断し、その情報をアドレス方向制御部(512)に伝える。また、同じ情報をアドレス比較器(510)にも伝える。アドレス比較器(510)は、CPU(102)内部の暗号処理アルゴリズムROM(106)、暗号処理ハードウェア(107)、RAM(108)が割り当てられているアドレスを把握しており、アドレスバス(504)又は、外部アドレスバス(507)から入力されるアドレスと比較する。

20 外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していると判断すると、アドレス比較器(510)はマイクロプロセッサからのアドレスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝え、外部バス制御信号を駆動させない。また、マスク信号生成部(511)にも伝え、信号マスク部(514)(519)にマスク信号を出力し、外部アドレスバス(507)、外部データバス(508)を駆動しないように制御する。もしくは、強制的にアドレスの値やデータの値を固定してしまう。

25 外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していないと判断すると、アドレス比較器(510)は外部

アドレスバスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝える。外部制御バス生成部(509)は、制御バス(503)へこのバスサイクルを伝達しない。もしくは、信号マスク部(514)(519)にマスク信号を出力し、アドレスバス(504)、データバス(505)を駆動しないように制御する。または、強制的にアドレスの値やデータの値を固定してしまう。

アドレスの値やデータの値を固定する方法として、第6図のように、信号マスク部(601)のゲート(602)と信号マスク部(603)のゲート(604)のように、ゲートの論理を変える事により実現できる。

このように、アドレス信号マスク回路で、RAM(108)領域以外の読み書きされても問題ない領域にアドレスを変換する事も可能である。

これにより、CPU(102)内部の処理をCPU(102)のバスであるシステムバス(114)を観察する事で推測する事が不可能になる。よって、CPU(102)内部で行う暗号処理の安全性が高まる。

次に第7図から第13図を用いて、鍵情報の取り扱いについて説明する。暗号化、複合化には鍵情報が必要であり、この鍵情報の秘匿化がシステム全体の安全性を高める。従来は、鍵情報を外部から与え、その鍵を人間が厳重に管理することで、システムの安全性を高めてきた。

本発明では、半導体内部で暗号化に必要な鍵情報を生成し、その情報は、半導体内部にのみ保持し、半導体外部に出力する場合は特定の相手にのみ分かる手段で出力することを特徴とする。鍵情報は乱数を用いて生成する。論理的に乱数を生成する場合、一般に疑似乱数として生成する。これは、ある種情報から複数の演算をくり返すことにより、離散した数値列を求めるものである。ところが、この疑似乱数は、種情報が同じであれば、同じ順序で離散した数列を生成してしまうため、種情報を入手すれば、同じ乱数を生成でき、再生可能乱数になってしまう。よって、種情報を厳重に

管理する必要性が生じる。そこで本発明では、種情報を必要としない乱数生成器(113)を設ける。

第7図は物理現象を用いて乱数を生成する乱数生成器(113)の構成例を示している。第7図では、乱数生成器(113)は、定電圧ダイオードやツェナーダイオードのノイズを元に乱数を生成する。第7図は、定電圧ダイオード(701)、抵抗(702)とコンデンサ(703)で構成されるローパスフィルタ(704)、コンパレータ(705)、フリップフロップ(706)で構成される。

定電圧ダイオード(701)は、信号波形(707)のようにノイズを発生する。このノイズは、定電圧ダイオード(701)の内部の半導体接合部分で生じる雪崩降伏がランダムに起きることに起因する物理現象である。このノイズをローパスフィルタ(704)を通すと信号波形(708)のように信号波形(707)の平均値に近い値をとる。この2つの信号をコンパレータ(705)に入力することにより、信号波形(709)のような、ランダムなパルス幅をもつ2値信号に変換することが出来る。この信号をさらにフリップフロップ(706)で半導体素子内の基準クロックに同期化させ、ランダムビット信号波形(710)を得る。

このランダムなビット列を必要なビットだけ、シフトレジスタに入力するなり、単位時間のパルスの数を計測するなりして乱数を得る。

これにより、乱数生成に種がいらず、再生不可能な乱数を得ることが出来る。また、ローパスフィルタ(704)により、ノイズを含む信号(707)の平均値(708)を求め、その平均値とノイズを含む信号を比較することにより、定電圧ダイオードの電圧に温度等による電圧変動等が生じてても、乱数生成に影響が及ばない乱数生成器を構成することが出来る。

第7図では、定電圧ダイオードをノイズ源として用いているが、物理現象に基づくノイズを発生する物であれば、これに限る物ではない。

第8図は、生成した鍵情報など秘密にしておく情報を格納する鍵保管領域の構成例を示している。第8図は、鍵保管領域(112)を、バッテリバック

アップされた SRAM で構成した例を示したものである。

本発明の CPU(102)を、SRAM(804)と SRAM 制御回路(809)、その他の CPU 内部論理ブロック(802)に分け、SRAM(804)と SRAM 制御回路(809)専用の電源(805)と、内部論理ブロック(802)用の主電源(803)をそれぞれ設ける。主電源(803)と鍵保管領域(112)用電源(805)は、タイオード(806)(807)を介して SRAM(804)の電源(808)として供給される。また、同じ電源(808)は SRAM 制御回路(809)の電源としても使用する。ゲート(810)は、内部論理ブロックで使用されている初期化信号(811)と主電源(803)とを監視し、主電源(803)へ電力が供給されておりなおかつ内部論理ブロックの初期化が終了するまで、SRAM(804)への信号を全て無効になるように固定する。これにより、鍵保管領域(112)にのみ電力を供給し、他の部分への電力供給を停止した状態でも、余分な漏れ電流等を無くすることができ、さらに電力供給を停止した部分に、ノイズ等が印加されたり、動作保証以下の電圧で誤動作したとしても、その影響を遮断することができる。ゲート(810)が“L”を出力すると、ゲート(812)は“L”を出力し、アドレス信号線(813)の電圧が何であっても変化しない。また、ゲート(815)も“L”を出力しバッファ(816)の出力インピーダンスを高くするため、データ信号線(814)へ漏れ電流を流すことがなくなる。また、ゲート(820)も“L”を出力するため、バッファ(821)の出力インピーダンスを高くするため、データ信号線(823)の電圧が何であっても、データ信号線(819)へ伝えることがない。また、ゲート(824)は“H”を出力し制御信号(826)を無効化して、SRAM の動作を止める。さらに、ゲート(810)(812)(815)(820)(824)、バッファ(821)を CMOS 構造の素子で構成することにより、入力信号(814)(817)(823)(822)(825)に流れる漏れ電流を微小に押さえることができるため、内部論理ブロック(802)への電力供給が停止しても、鍵保管用電源(805)の電力が漏れ出ることはない。これにより、鍵保管用電源(805)から消費する電力を必要最小限に抑えることができ、

バックアップバッテリー (828) の寿命を長くすることができる。

主電源 (803) から電力が供給され、内部論理ブロック (802) の初期化が終了すると、ゲート (810) は "H" を出力する。すると、ゲート (812) は、アドレス信号線 (813) のデータをアドレス信号線 (814) に伝える。ゲート (815) は、
5 SRAM 読み出し信号 (817) が有効なときにバッファ (816) を有効にしデータ信号線 (819) のデータをデータ信号線 (818) に伝える。ゲート (820) は、SRAM 書き込み信号 (822) が有効なときにバッファ (821) を有効にしデータ信号線 (823) のデータをデータ信号線 (819) に伝える。ゲート (824) は、制御信号線 (825) のデータを制御信号線 (826) へ伝える。これにより、正常に
10 SRAM (804) をアクセス可能になる。

また、CPU (102) を収納する筐体等のケースに各種感知器を設け、それらからの信号を元に、バッテリー (828) から供給される鍵保管用電源 (805) を制御する異常検出器 (827) を設ける。筐体等のケースの分解、解体等の異常を検出したときに、SRAM (804) への電力供給を停止し、鍵情報を消失させてしまうものである。さらには、主電源 (803) から電力が供給されている場合には、異常検出器 (827) が作動して、鍵保管用電源 (805) からの電力供給を
15 絶っても、主電源 (803) から SRAM (804) へ電力が供給されてしまうため、異常検出信号 (829) を内部論理ブロック (802) に入力し、異常を伝え、動作を制限または停止させる。

20 CPU (102) 内で、SRAM (804) への電源を統合してもよいが、主電源とバッテリーからの電力を、異常検出器 (827) 内で統合し、いかなる場合でも異常を検出したら、SRAM (804) へ電力が供給を絶つ構成にしてもよい。

異常検出器 (827) と CPU (102) を接続する信号線および電源線は極力短くかつ基板の内部を通す等、簡単には探針不可能なように実装する必要がある。さらに、配線箇所異なる、複数の信号線で接続する等、防御手段を
25 講じる必要がある。これにより、装置を分解されても秘密鍵が半導体素子

外部に漏れることがなくなる。

本発明で生成する鍵は、半導体自体を識別する為に必要な鍵と、情報を暗号化するのに用いる鍵の２種類あり、それぞれ使用目的が異なる。前者を認証用の鍵、後者を情報暗号化の為に用いる鍵とする。頻繁に鍵を生成する必要がある鍵は、情報暗号化の為に用いる鍵であり、基本的には情報暗号化の度に生成する。認証用の鍵は、月単位や年単位といった定められた期間毎に生成し、半導体自体を識別する情報として用いる。

第 9 図は、暗号化した装置と復号化する装置が同一である場合の、暗号化鍵と復号化鍵の取り扱いを示したものである。

半導体である CPU(102) 内部で生成した情報(901)を暗号化し、外部記憶装置(104)等に暗号化ファイル(116)として格納し、再び CPU(102)内部で使用するために復号化する場合、鍵情報(902)は CPU(102)内部にのみ存在すれば良い。暗号化ファイル(113)(116)をこの CPU(102)でのみ扱えるようにするためには、鍵情報(902)を CPU(102)内部の乱数生成器(113)で生成し、鍵保管領域(112)にのみ保管しておく。

また、複数の情報(903)、(905)に対して暗号化する場合に、それぞれ異なる暗号鍵(904)、(906)を用いる場合は、それぞれの鍵情報(904)、(906)を鍵保管領域(112)に保管する必要がある。

図では、メモリ(108)内で暗号化処理と復号化処理を行う構成を図示しているが、CPU(102)内の処理であれば、暗号アルゴリズム(106)を用いた方法でも、暗号処理ハードウェア(107)を用いた方法でも良い。

また、第 10 図に示したように、鍵保管領域(112)内には、予め乱数生成器(113)で生成した鍵(1001)のみを保管し、情報(1002)(1003)を暗号化する度に、それぞれの情報に対応して生成した鍵(1004)(1005)を鍵(1001)で暗号化し、暗号化鍵(1006)(1007)を作る。情報(1002)(1003)は、それぞれ鍵(1004)(1005)を用いて暗号化し、暗号化ファイル(1008)(1009)を生成する。

このようにして、生成した暗号化ファイル(1008)と暗号化鍵(1006)とをまとめてファイル(1010)として外部記憶装置格納し、生成した暗号化ファイル(1009)と暗号化鍵(1007)とまとめてファイル(1011)として外部記憶装置格納することで、鍵保管領域(112)に格納する鍵情報を削減しても良い。

5 第1図は、情報を暗号化する装置と暗号化された情報を復号化する装置が異なる場合の鍵の取り扱いを示したものである。この場合、相手が正しいか否か確認する事が必要になる。これを、相手を認証と呼ぶ。

相手を認証する手段としては、非対象鍵暗号を用いて行う。非対象鍵とは、情報を暗号化し暗号文にする鍵と暗号文を復号化し情報に戻す鍵が異なる暗号をさす。非対称鍵暗号は公開鍵暗号とも呼ばれ、暗号化鍵と復号化鍵の2つの鍵のうち片方を公開し、もう一方は秘密にして用いる。暗号化鍵で暗号化した情報は、対応する復号化鍵のみで復号化が可能である。つまり、二つの鍵のうち、公開する方を公開鍵、秘密にする方を秘密鍵とすると、公開鍵で暗号化した暗号文は、秘密鍵でのみ復号可能であり、秘密鍵で暗号化した暗号文は、公開鍵でのみ復号可能である性質を持つ。これを用いることにより、特定の相手にのみ解る手段で情報を送る事や、発信者を特定する事が可能になる。

20 特定の相手にのみ情報を送りたい場合は、相手の公開鍵を入手し、相手の公開鍵を用いて送りたい情報を暗号化する。このようにして出来た暗号文は、同じ公開鍵では復号化できず、相手が秘密にしている秘密鍵でのみ復号化が可能な暗号文となる。これにより、特定の相手にのみに情報を伝達する事が可能になる。一般には、非対称暗号(公開鍵暗号)は処理が複雑で、時間も必要とする事から実際の情報の暗号は、対称鍵暗号(共通鍵暗号)で暗号化し、この暗号化で使用する鍵を毎回乱数より生成し、この鍵情報を非対称鍵暗号(公開鍵暗号)を用いて、相手に秘密裏に送る方法をとる。

25 送信者を特定する方法は、情報を送る側が情報そのものまたは、情報に

対応する情報(ダイジェスト等)を秘密鍵で暗号化した暗号化情報を相手に送る。相手は、送信側の公開鍵を入手し、送られてきた暗号化情報を送信側の公開鍵で復号化し、正当な内容と判断することで、送信側のみが所有する秘密鍵で暗号化されていたと判断し、送信側が正当であると判断出来る。

第 1 1 図において、装置 A(1101a)および装置 B(1101b)では、予め各々の装置自身が装置識別情報として、公開鍵(1104a)(1104b)と秘密鍵(1105a)(1105b)を生成しておく。これらの鍵は、剰余演算を用いた公開鍵暗号では、二つの素数積を用いて生成される。素数は乱数生成(1102a)(1102b)し、その乱数が素数であるか否かを判断し生成する(1103a)(1103b)。ここで生成した鍵は、半導体自体を識別する為に必要な鍵である。

ここで、情報(1116)を装置 A(1101a)から装置 B(1101b)へ送る事を考える。

装置 A(1101a)から装置 B(1101b)にのみ解釈出来る手段で、情報(1116)を送るためには、情報(1116)を暗号化して送る事になるが、その時に使用する鍵は、その時のみ有効で、他の情報転送時には他の鍵を使用した方が、万が一鍵情報が漏洩しても被害を最小限にくい止める事ができる。その為には、毎回生成する情報(1116)を暗号化する共通鍵(1111)を、装置 B にのみ伝えなければならない。

これを実現するためには、まず装置 A(1101a)は、装置 B を(1101b)へ公開鍵転送要求(1106)を出す。これをうけて、装置 B を(1101b)は装置 B 公開鍵(1104b)を装置 A(1101a)へ転送する(1107)。装置 A(1101a)は、乱数を生成し(1109)、その乱数を元に共通鍵(1111)を生成する(1110)。生成した共通鍵(1111)を、装置 B(1101b)から受け取った、装置 B 公開鍵(1108)を公開鍵暗号化し(1112)、暗号化鍵情報(1113)を生成する。また、共通鍵(1111)

で情報(1116)を共通鍵暗号化(1115)し、暗号化情報(1117)を生成する。この暗号化鍵情報(1113)と暗号化情報(1117)を送ることにより、装置 B にのみ解釈可能な状態で、情報(1116)を送る事ができる。装置 B(1101b)では、受け取った暗号化鍵情報(1119)を装置 B 秘密鍵(1105b)で公開鍵復号化し(1120)、共通鍵(1121)を取り出し、この共通鍵(1121)で受け取った暗号化情報(1122)を共通鍵復号化し(1123)、情報(1124)を得る。

さらに、情報転送(1118)が装置 A(1101a)から送られた事を証明するためには、第 1 2 図のように、情報(1116)のダイジェストをハッシュ関数(1201)を用いて、ハッシュ値(1102)として求め、このハッシュ値(1102)を、装置 A 秘密鍵(1105a)で公開鍵暗号化し(1203)、暗号化ハッシュ値(1204)を生成する。装置 A 公開鍵(1104a)を装置 B(1101b)へ転送し(1205)、暗号化ハッシュ値(1204)を装置 A(1101a)の署名として転送する(1206)。装置 B(1101b)では、受け取った装置 A 公開鍵(1207)を用いて、暗号化ハッシュ値(1208)を公開鍵復号化し(1209)、装置 A(1101a)で生成したハッシュ値(1210)を得る。一方、受け取った情報(1124)から、ハッシュ関数(1211)を用いて、ハッシュ値(1212)を求める。この二つのハッシュ値(1210)(1212)を比較し(1213)、結果が同じであれば、情報(1124)の送り主を装置 A(1101a)と確認する事ができる。

第 1 2 図では、情報(1116)のハッシュ値を求める方法を示したが、情報(1116)のデータの大きさが小さい場合、情報そのものを装置 A 秘密鍵(1105a)で暗号化し、装置 A 公開鍵(1104a)と共に転送しても良い。

相手の公開鍵を入手する方法は、図に示したように、相手から入手しても良いし、相手と利害関係のない第三者から入手仕手も良い。

ここで、相手から公開鍵を入手する場合に、入手した公開鍵が本当に正しいか、他人が相手に成り済ましていないかを確認する必要が生ずる。

第 1 3 図は、第 1 1、1 2 図において相手から受け取った公開鍵が本当

に正しいか否かを確認する手段を示したものである。第 1 3 図は、各装置を認証する認証局として、装置 C(1301)を設けた構成をとったものである。装置 C(1301)は、システムに参加する各装置の公開鍵を認証する。そのために、装置 C(1301)内部で乱数生成し(1302)、その乱数から素数を生成し(1303)、装置 C の公開鍵(1304)と秘密鍵(1305)を生成しておく。この装置 C の秘密鍵がシステム内で最も機密にしなければならない情報になる。

装置 A(1101a)、装置 B(1101b)で、装置識別用に生成した公開鍵(1104a)(1104b)と秘密鍵(1105a)(1105b)の内、それぞれの公開鍵を装置 C(1301)に対して、認証依頼として転送する(1316a)(1316b)。認証依頼を受けた装置 C(1301)は、受け取った各装置の公開鍵(1306a)(1306b)を、装置 C の秘密鍵(1305)で公開鍵暗号化し(1307a)(1307b)、認証書(1308a)(1308b)を生成する。この認証書と装置 C の公開鍵(1304)を一緒にした認証結果(1309a)をそれぞれの装置へ転送する(1317a)(1317b)。

各装置は、自分の公開鍵の認証書を記憶しておく。情報転送の為の公開鍵要求がきたら、自分の公開鍵(1105b)を転送すると共に、認証書も転送し、自分装置 C によって、認証されている事を示す。受け取った認証書(1312)は、記憶してある装置 C の公開鍵を用いて、公開鍵復号化される(1313)。認証書(1312)内の装置 B の公開鍵(1314)を取り出し、装置 B(1101b)から転送された公開鍵(1108)と比較する(1315)ことにより、装置 B の公開鍵の正当性を検証する。

装置 C による認証作業における装置とその公開鍵の対応は、電子的な確認だけでなく、装置に改良等第三者の手が加えられていないか等、細かい検査ののちに行われるものである。

このような、手順を踏むことにより相手から、公開鍵を入手しても正当性を確認する事が可能になる。

次に、本発明の第四の実施例を、第 1 4 図を用いて説明する。

第 1 4 図は、一般的な情報処理装置の構成を模式的に表した図である。情報処理装置 (1401) は、複数の半導体部品から構成されている。CPU (1402) はプロセッサバス (1404) で、キャッシュメモリと主記憶制御部 (1405) に接続
5 される。主記憶制御部 (1405) は、システムバス制御部を含み、メモリバス (1413) とシステムバス (1407) が接続される。メモリバス (1413) には、主記憶装置 (1406) が接続され、システムバス (1407) には、外部記憶装置 (1408)、表示系制御部 (1410)、通信系制御部 (1411)、その他 I/O 制御部 (1412) が接続される。表示系制御部 (1410) は、専用バスで主記憶装置制御部 & システムバス制御部 (1405) に接続されていても良い。外部記憶装置制御部 (1408)
10 には、外部記憶装置 (1409) が接続される。

主記憶装置 (1406) のアドレス領域と、システムバス (1407) に接続される各部分のアドレス領域は異なっているため、アドレスでアクセスすべき領域を判断し、主記憶装置制御部 & システムバス制御部 (1405) が切り替えて
15 いる。

このような、情報処理装置 (1401) では、情報処理装置を一つのシステムと捉えたと、このシステム内の主となるプロセッサは、CPU (1402) である。この CPU 内部で暗号化処理を閉じさせる。例えば、CPU (1402) を第 1 図のように、マイクロプロセッサ (105) と、暗号処理アルゴリズム ROM (106) と、
20 暗号処理ハードウェア (107) と、RAM (108) と、鍵保管領域 (112) と、外部バス制御部 (109) で構成し、さらに、同一半導体チップ上に集積する。また、本発明は、第 1 9 図および第 2 0 図に示すとおり、複数の CPU を有する情報処理装置であってもよい。

本発明の第五の実施例を第 1 5 図を用いて説明する。

第 1 5 図は、情報処理装置が他の情報処理装置と接続され、通信可能である構成を示す図である。ここでは、第 1 図の外部記憶装置の代わりに、
25

通信系制御部を設けた構成をとる。なお、通信系制御部は、情報処理装置の外に接続されていてもよい。

情報処理装置(1501)は、CPU(1502)と、通信系制御部(1503)とを備え、システムバス(1514)で接続される。CPU(1502)は、マイクロプロセッサ(1505)、暗号処理アルゴリズム ROM(1506)、暗号処理ハードウェア(1507)、RAM(1508)、外部バス制御部(1509)、鍵保管領域(1512)から構成され、マイクロプロセッサバス(1510)で接続される。

第15図では、情報処理装置は、CPUと通信系制御で構成されているが、他に主記憶や外部記憶装置等が備わっていても良い。通信系制御部(1503)を経由した通信回線(1504)の先に、外部記憶装置と同じ機能を持つ装置が接続されていても良いし、情報処理装置が接続されていても良い。

但し、通信回線(1504)の先に接続される装置が、記憶装置か情報処理装置かで、暗号の掛け方が異なる。

通信回線の先に接続される装置が、外部記憶装置の場合、データを暗号化し、それを記憶装置に格納し、暗号化されたデータを記憶装置から読み出して復号化するものである。このため、暗号化に用いた鍵は、暗号化を行った情報処理装置のCPUだけが保持していれば良い。

通信回線の先に接続される装置が、情報処理装置の場合、通信回線を挟んで情報処理装置Aと情報処理装置Bが存在する。この場合、情報処理装置Aで情報を暗号化し、情報処理装置Bで情報を復号化する状況が生ずる。大量のデータを高速に暗号化／復号化するためには、共通鍵暗号系が適する。しかし、暗号化と復号化で同じ鍵を用いるため、情報処理装置AとBで、同じ鍵を所有していなければならない。この同じ鍵を、情報処理装置AとBであらかじめ設定しておいても良いし、暗号化したデータを送る前に、情報処理装置AとBで相互認証を行い、暗号化に用いた鍵を共有する方法を取っても良い。相互認証にも暗号処理が用いられるため、これらの

処理は、CPU 内部で処理される。

この情報処理装置 A と B がネットワークを介して接続されている様子を第 23 図に示す。

5 RAM(1508)内で、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信系制御部(1503)に転送する事により、安全な通信が可能になる。RAM(1508)内で暗号化したデータを通信系制御部(1503)に転送し、通信系制御部(1503)において、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信路(1504)にデータを送出しても良い。

10 本発明の第六の実施例を第 16 図、第 17 図、第 18 図、第 21 図および第 22 図を用いて説明する。

第 16 図は、磁気ディスク(1601)等の外部記憶装置群を、ディスクシステムコントローラ(1602)が制御する構成を取り、ディスクシステムコントローラ(1602)は、上位の情報処理装置であるホストシステム(1603)に接続されている。

15 磁気ディスク(1601)内には、ファイルとして記憶されているデータと、そのファイルが磁気ディスク上の何処に格納されているかを示すファイル配置情報がある。PC 等の小型情報処理装置では、ファイルとファイル配置情報を管理するファイルシステムプログラムを、小型情報処理装置の CPU が処理する場合もあるが、高速動作や高信頼性を実現するディスクシステムコントローラでは、ディスクシステムコントローラ自体がファイルとファイル配置情報を管理する場合もある。

20 本実施例は後者に適用したものである。ホストシステム(1603)では、ファイル(1604)とファイル識別子(1605)で管理する。ファイル(1604)が暗号化されてるか否かは、ホストシステムに依存し、ディスクシステムコントローラでは関知しなくて良い。ディスクシステムコントローラ(1602)では、磁気ディスク(1601)上のファイル配置情報(1606)を暗号化して管理す

る。

本実施例での、ホストシステムが暗号化した暗号化ファイル(1607)を読み出すまでの動作を説明する。

まず、ホストシステムは、必要とする暗号化ファイルに対応するファイル識別子(1605)をディスクシステムコントローラ(1602)に送り、暗号化ファイルの読み出し要求を行う。読み出し要求を受けたディスクシステムコントローラ(1602)は、磁気ディスク(1601)から、暗号化されたファイル配置情報(1606)を読み出し、ディスクシステムコントローラ(1602)内で復号化し、ファイル配置情報(1608)を取り出す。このファイル配置情報(1608)内からファイル識別子(1605)を検索し、実際のファイルの配置情報を得る。選ばれたファイル配置情報を用いて、要求された暗号化ファイル(1607)を磁気ディスク(1601)から読み出し、ホストシステム(1603)へ転送する。

磁気ディスクにファイルを書き込む場合を第10図で説明する。ファイル配置情報(1608)を得るまでは、前記暗号化ファイルの読み出し動作と同じである。ファイル配置情報(1608)から、磁気ディスク(1601)の空き状態を確認し、磁気ディスク(1601)空き領域に暗号化ファイル(1604)を書き込む。書き込み終了後、ファイル配置情報(1608)を更新し、暗号化した後、磁気ディスク(1601)に暗号化ファイル配置情報(1701)として書き込む。

第18図で、ディスクシステムコントローラの構成を説明する。

本発明のディスクシステムコントローラ(1801)は、内部にディスクシステムのCPU(1802)と、磁気ディスクインタフェース(1813)と、ホストシステムインタフェース(1804)を持ち、CPU(1802)は、マイクロプロセッサ(1805)と、暗号処理アルゴリズムROM(1806)と、暗号処理ハードウェア(1807)と、RAM(1808)と、鍵保管領域(1811)と、外部バス制御部(1809)と、乱数生成器(1820)で構成される。

なお、第 2 1 図および第 2 2 図に示す通り、1 台の情報処理装置に複数の磁気ディスク装置が接続される構成としてもよい。

このような、ディスクシステムコントローラを用いる事により、磁気ディスク内の情報を全て暗号化する事が可能になり、情報保管時の安全性が高まる。

本発明の暗号処理ハードウェアは、暗号化と復号化において共通の鍵を用いる共通鍵暗号では、専用のハードウェアであり、ローテータ、加算器、論理演算器等で構成される。共通鍵暗号としては、あるデータ長を単位に、ビットのローテートと加算と論理演算を主演算とした暗号化手段である Multi 系の暗号、M6 暗号等を用いる事も出来る。

公開鍵暗号を用いる場合は、演算量の大きい剰余演算器を専用のハードウェアとして設ける。

産業上の利用可能性

本発明によれば、情報処理装置内のシステムバスやプロセッサバスにも秘密情報を出さずに、暗号処理が可能になる。暗号処理とその処理に関する秘密情報、暗号アルゴリズム、途中経過、鍵情報等が、同一半導体内で処理されるため、秘密保持効果が高い情報処理装置を構築できる。

請 求 の 範 囲

1. 情報に対して所定の処理を施す制御装置と、

5 前記制御装置と当該情報処理装置を構成する他の装置を接続するバスを有する情報処理装置において、

前記制御装置は、鍵情報を生成し、暗号化すべき情報の暗号化を、当該制御装置を含む半導体チップ内で実行することを特徴とする情報処理装置。

2. 請求項 1 に記載の情報処理装置において、

10 前記制御装置は、暗号化されていない情報の前記バスへの出力を抑止する外部バス制御装置を有することを特徴とする情報処理装置。

3. 請求項 2 に記載の情報処理装置において、

前記外部バス制御装置は、暗号化しなくともよい情報は、前記バスへ出力することを特徴とする情報処理装置。

15 4. 請求項 1 に記載の情報処理装置において、

前記制御装置で暗号化された情報を格納する記憶装置を有することを特徴とする情報処理装置。

5. 請求項 1 に記載の情報処理装置において、

20 前記制御装置は、情報の書き込みの際に、暗号化された情報を復号化する手段を有することを特徴とする手段を有することを特徴とする情報処理装置。

6. 請求項 5 に記載の情報処理装置において、

25 ネットワークを介して他の情報処理装置と接続され、他の情報処理装置で暗号化されて送信された情報を前記制御装置で復号化することを特徴とする情報処理装置。

7. 請求項 1 に記載の情報処理装置において、

前記処理装置を複数個有し、夫々の処理装置にて暗号化を行うことを特徴とする情報処理装置。

8. 請求項 1 に記載の情報処理装置において、

前記処理装置は、暗号化されたプログラムを受信し、復号化を施す手段を有することを特徴とする情報処理装置。

9. 請求項 1 に記載の情報処理装置において、

前記処理装置は、前記所定の処理を実行するマイクロプロセッサと、前記情報の暗号化処理のアルゴリズムが格納された暗号処理アルゴリズム格納装置と、

前記アルゴリズムに従って暗号化処理を実行する暗号化装置と、前記マイクロプロセッサ、暗号処理アルゴリズム格納装置および前記暗号化装置それぞれを接続するマイクロプロセッサバスとを有することを特徴とする情報処理装置。

10. 情報を処理する処理装置を有し、暗号化された暗号化情報を格納する磁気ディスクを制御するディスクシステムコントローラにおいて、

前記暗号化情報の読み出し要求を受け取った場合、鍵情報を生成し、前記磁気ディスクに格納された情報の配置を示す暗号化されている暗号化ファイル配置情報を、前記磁気ディスクから読み出し、読み出した暗号化ファイル配置情報を前記処理装置を含む半導体チップ内で復号化し、復号化されたファイル配置情報に基づいて、前記暗号化情報を読み出すことを特徴とするディスクシステムコントローラ。

11. 請求項 10 に記載ディスクシステムコントローラにおいて、

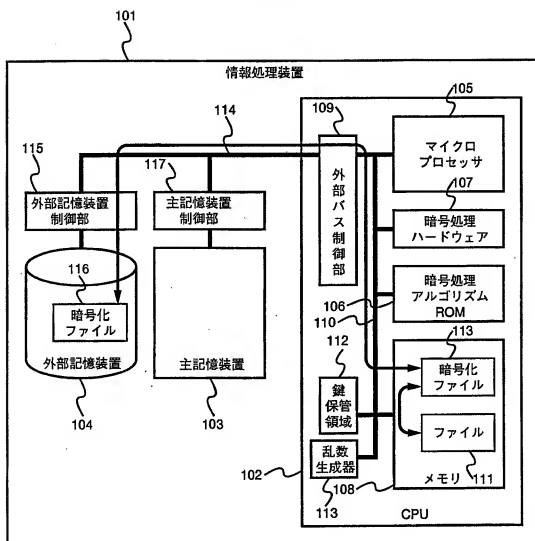
当該ディスクコントローラは、複数の磁気ディスクに接続されていることを特徴とするディスクシステムコントローラ。

12. 請求項 10 に記載ディスクシステムコントローラにおいて、

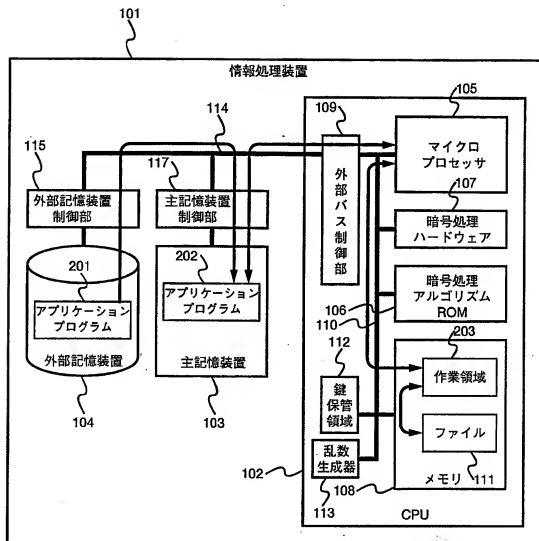
当該ディスクシステムコントローラは、情報処理装置に接続されており、

前記情報処理装置からの要求により、前記暗号化情報を読み出すことを特徴とするディスクシステムコントローラ。

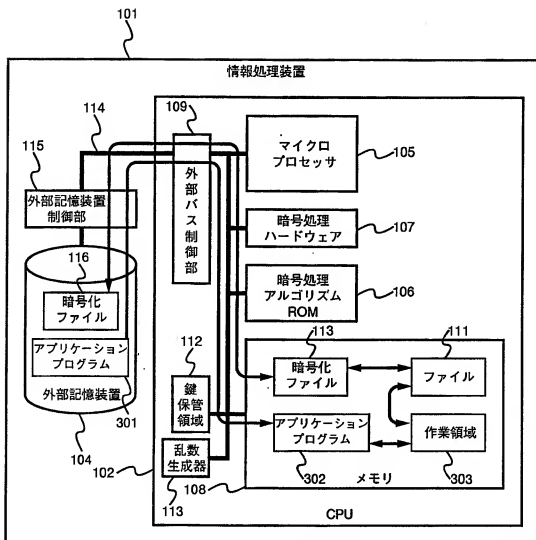
第1図



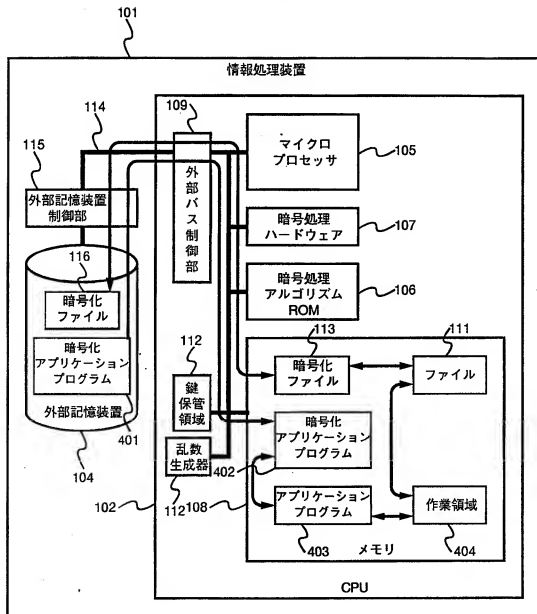
第 2 図



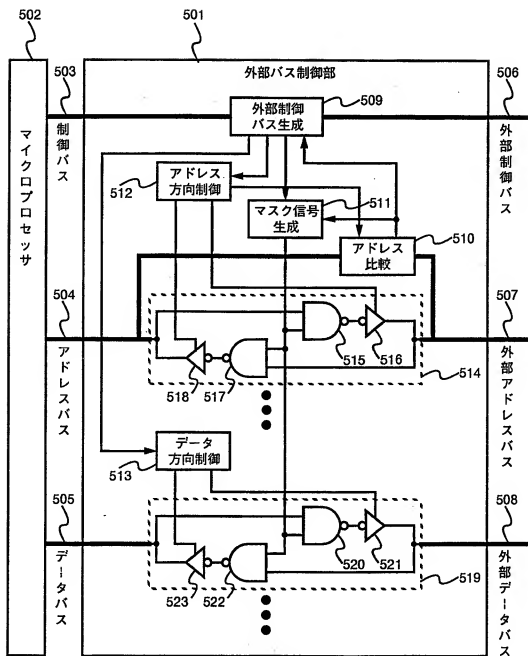
第3図



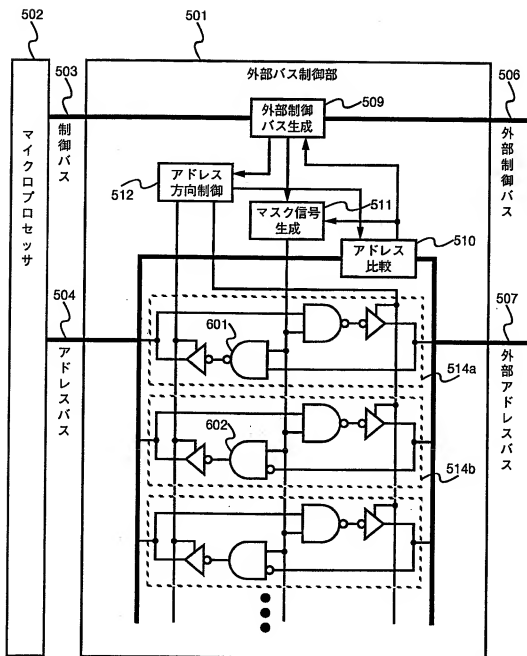
第 4 図



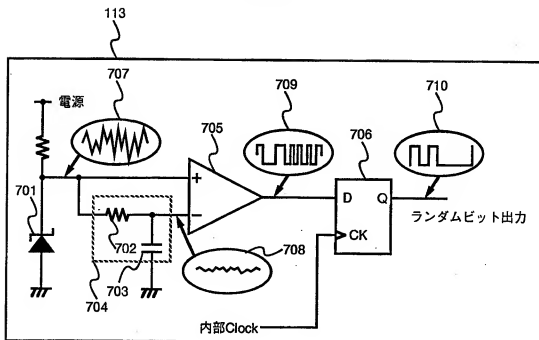
第 5 図



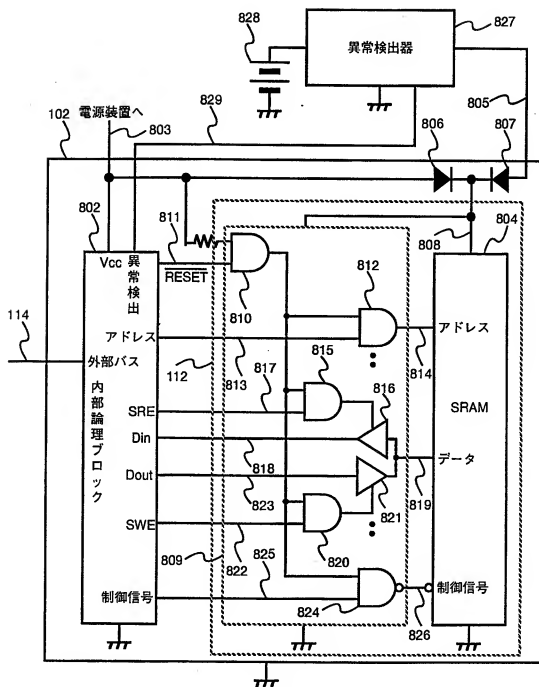
第6図



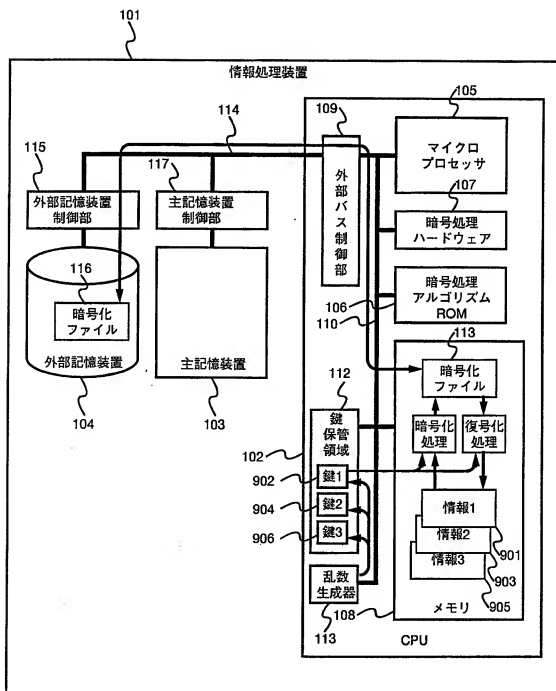
第 7 図



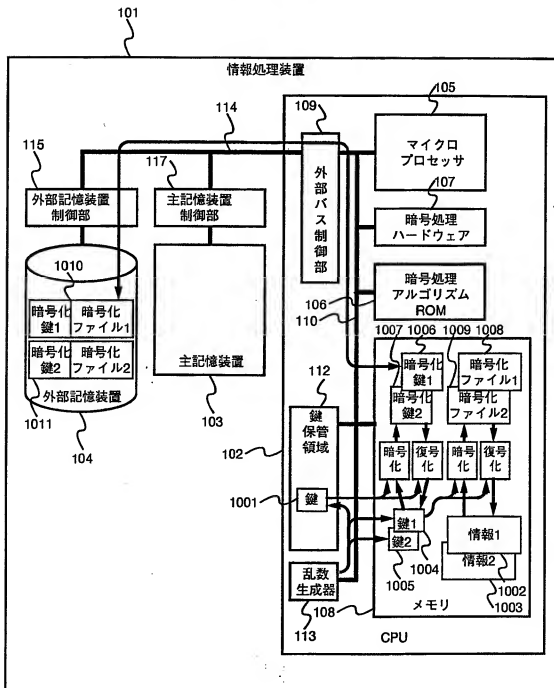
第 8 図



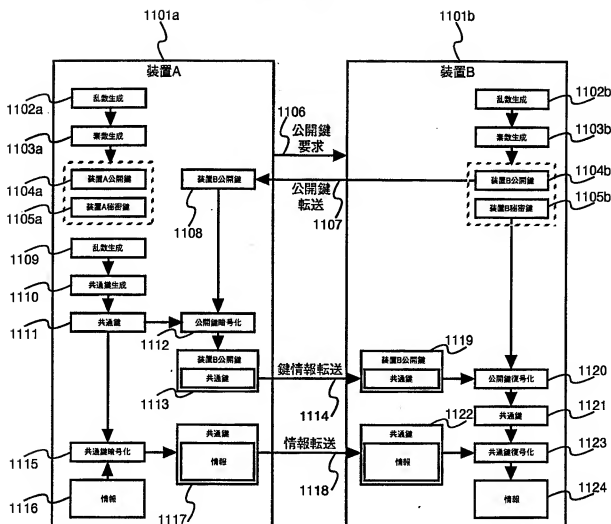
第9図



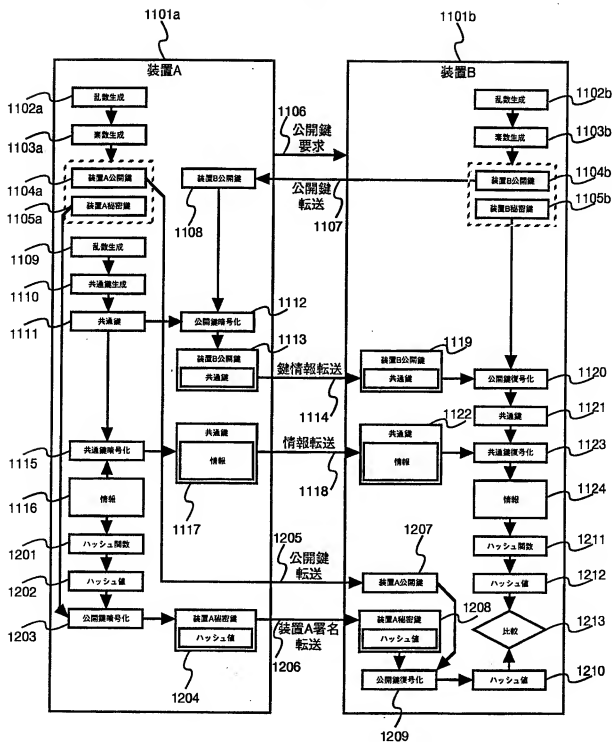
第10図



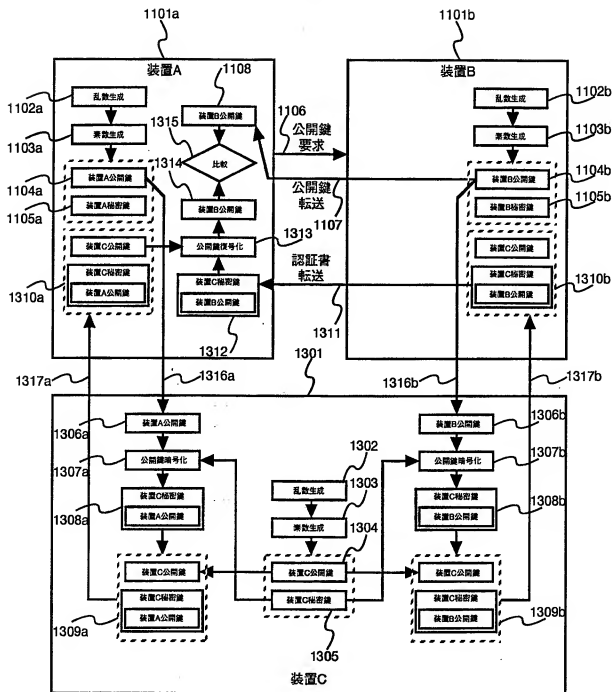
第 1 1 図



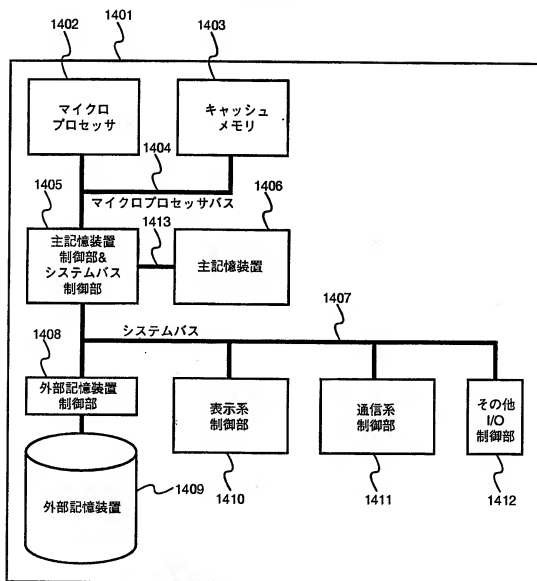
第12図



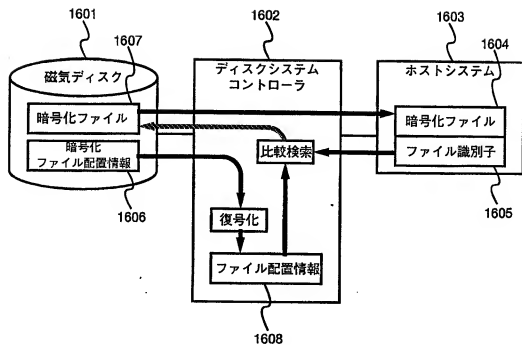
第 1 3 図



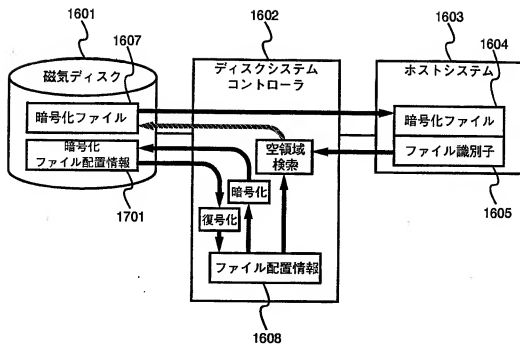
第 1 4 図



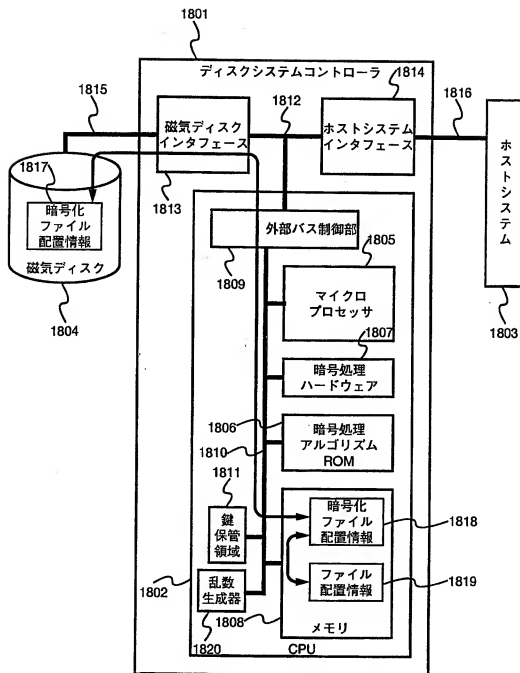
第 1 6 図



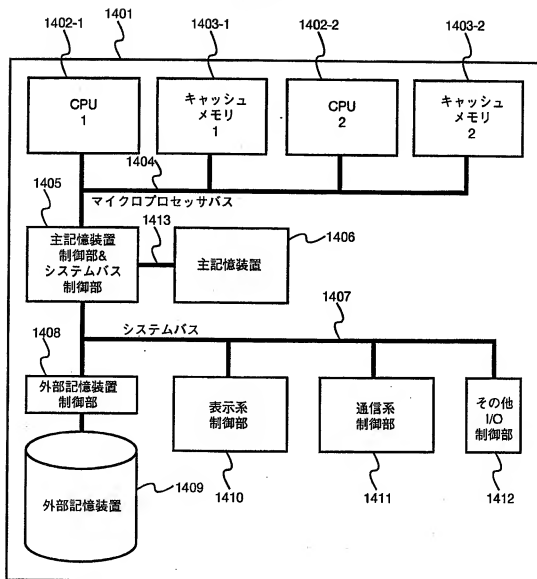
第17図



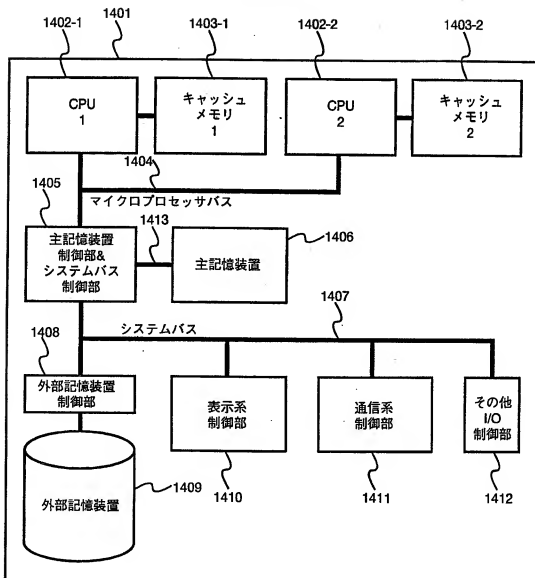
第 18 図



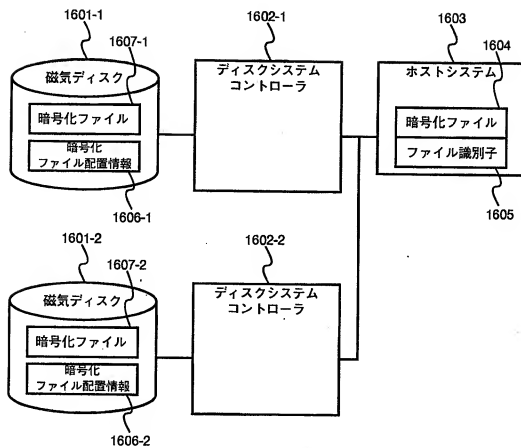
第 19 図



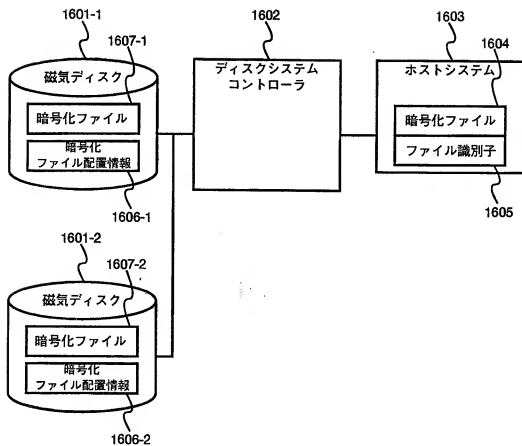
第 20 図



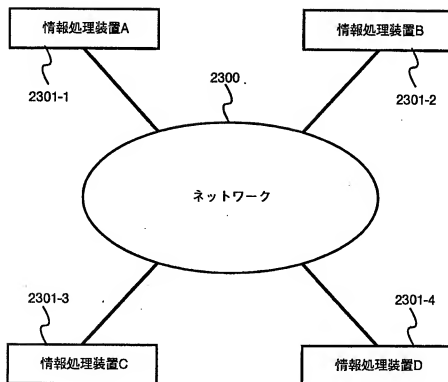
第 2 1 図



第 2 2 図



第 2 3 図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/01333

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Kokai Jitsuyo Shinan Koho 1971-2000

Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 05-053921, A (Nippon Steel Corporation),	1-9
Y	05 March, 1993 (05.03.93) (Family: none)	10-12
X	JP, 64-041947, A (Hitachi, Ltd., Hitachi Tobu	1-9
Y	Semiconductor K.K.),	10-12
	14 February, 1989 (14.02.89) (Family: none)	
Y	JP, 04-163768, A (Hitachi, Ltd.),	10-12
	09 June, 1992 (09.06.92) (Family: none)	
Y	JP, 09-044407, A (NEC Eng. Ltd.),	10-12
	14 February, 1997 (14.02.97) (Family: none)	
A	JP, 04-149652, A (Mitsubishi Electric Corporation),	1-12
	22 May, 1992 (22.05.92) (Family: none)	
A	JP, 02-297626, A (NEC Corporation),	1-9
	10 December, 1990 (10.12.90) (Family: none)	
A	JP, 05-314014, A (Toshiba Corporation),	10-12
	26 November, 1993 (26.11.93) (Family: none)	

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search
19 May, 2000 (19.05.00)Date of mailing of the international search report
13 June, 2000 (13.06.00)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JP00/01333

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996
 日本国実用新案登録公報 1996-2000
 日本国公開実用新案公報 1971-2000

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 05-053921, A (新日本製鐵株式会社)	1-9
Y	5. 3月. 1993 (05. 03. 93), (ファミリーなし)	10-12
X	JP, 64-041947, A (株式会社日立製作所, 日立東部 セミコンダクタ株式会社)	1-9
Y	14. 2月. 1989 (14. 02. 89), (ファミリーなし)	10-12
Y	JP, 04-163768, A (株式会社日立製作所) 9. 6月. 1992 (09. 06. 92), (ファミリーなし)	10-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリ

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

19. 05. 00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

梅村 助樹



5N 7313

電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 09-044407, A (日本電気エンジニアリング株式会社) 14. 2月. 1997 (14. 02. 97), (ファミリーなし)	10-12
A	J P, 04-149652, A (三菱電機株式会社) 22. 5月. 1992 (22. 05. 92), (ファミリーなし)	1-12
A	J P, 02-297626, A (日本電気株式会社) 10. 12月. 1990 (10. 12. 90), (ファミリーなし)	1-9
A	J P, 05-314014, A (株式会社東芝) 26. 11月. 1993 (26. 11. 93), (ファミリーなし)	10-12